# ON ALGEBRAIC CLOSURE IN PSEUDOFINITE FIELDS

ÖZLEM BEYARSLAN, EHUD HRUSHOVSKI

Abstract. We study the automorphism group of the algebraic closure of a substructure $A$ of a pseudo-finite field $F$. We show that the behavior of this group, even when $A$ is large, depends essentially on the roots of unity in $F$. For almost all completions of the theory, we show that algebraic closure agrees with definable closure, as soon as $A$ contains the relative algebraic closure of the prime field.

## 1. Introduction

A pseudofinite field is an infinite model of the theory of finite fields. By Ax [**Ax**], we know that a field $F$ is pseudofinite if and only if it is 1) perfect, 2) PAC and 3) has a unique (and so necessarily Galois and cyclic) extension in the algebraic closure $F^a$ of $F$ of degree $n$ for every $n \in \mathbb{N} \setminus \{0\}$. See [**FJ**] for the PAC property; it will play almost no role in this paper.

We are interested in definable and algebraic closure in $F$, over a substructure $A$ containing an elementary submodel. This is a problem about embeddings of function fields into $F$. Surprisingly, the answer depends intimately on embeddings of number fields, or finite fields, into $F$. Say the characteristic is zero. We show in particular that algebraic closure and definable closure coincide if and only if, for each prime $p$, the cyclotomic field of $p^n$'th roots of unity is contained in a finite extension of $F$.

Real closed fields provide a geometrically comprehensible way of symmetry-breaking in algebraic geometry; a Galois cover of an algebraic variety splits into semi-algebraic sections. Our results imply that pseudo-finite fields give an alternative, but equally geometric approach to such a splitting: the Galois cover splits into definable sections.

The results above are in fact valid for quasi-finite fields in the sense of [**S**], p. 188, i.e. perfect fields with absolute Galois group $\hat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$. We use pseudo-finiteness only in order to demonstrate the converse, that if the field of of $p^n$'th roots of unity is contained in a finite extension of $F$, then Galois groups of order divisible by $p$ occur geometrically in models of the theory.

## 2. Quasi-finite Fields

We write $\leq$ for the substructure relation; in particular, for fields $A, B$, $A \leq B$ means that $A$ is a subfield of $B$.

By definition, a quasi-finite field $F$ has a unique extension in $F^a$ of degree $n$ for every $n \in \mathbb{N}\setminus\{0\}$. Let $F_n$ denote the unique extension of $F$ in $F^a$ of degree $n$. This extension is easily seen to be interpretable in $F$ using parameters from $F$. Indeed, as $F$ is perfect, $F_n = F(\alpha)$ for some $\alpha \in F_n$. Let $X^n + a_1X^{n-1} + \cdots + a_n$ be the minimal polynomial of $\alpha$ over $F$. Then $F_n$, which is an $n$-dimensional vector space over $F$ with basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$, is definably isomorphic to $F^n$ via this basis as a vector space. Also any linear homomorphism of $F_n$ translates into a definable (with

*Date*: September 11, 2009.

The second author was supported by ISF 1048/07.

parameters) linear homomorphism of $F^n$ (coded by an $n \times n$ matrix over $F$). In particular, the $\alpha$-multiplication in $F_n$, the multiplicative structure of $F_n$ and the action of $\mathrm{Gal}(F_n/F)$ on $F_n$ can all be definably(with parameters) coded in $F^n$.

Note that to interpret $F_n$ in $F$ we only need $a_1, \ldots, a_n$ as parameters, but to interpret the action of an element $\tau$ of $\mathrm{Gal}(F_n/F)$ in $F$, apart from these $n$ parameters, we also need $b_0, \ldots, b_{n-1} \in F$ where $\tau(\alpha) = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$, which makes up a total of $2n$ parameters. Note also that any other choice of the parameters $a_1, \ldots, a_n$ for which the polynomial $X^n + a_1X^{n-1} + \ldots + a_n$ is irreducible gives rise to an isomorphic structure $F_n$; on the other hand, different choices of the parameters $b_0, \ldots, b_{n-1}$ may define different field automorphisms.

**Lemma 1.** *Let $F$ be a quasi-finite field and $\sigma$ be a topological generator of $\mathrm{Aut}(F^a/F)$, let $M$ be an elementary submodel of $F$. Let $\mu$ be in $\mathrm{Aut}(F/M)$ then any extension of $\mu$ to $F^a$ commutes with $\sigma$.*

**Proof:** It is enough to show that $\sigma$ and $\mu$ commute on $F_n$ where $F_n$ is the unique extension of $F$ of degree $n$. Since $M$ is an elementary submodel of $F$, $F_n = F(\alpha)$ where $\alpha$ is a root of an irreducible polynomial of degree $n$ with coefficients in $M$. We will show that $\sigma\mu(\alpha) = \mu\sigma(\alpha)$. We know that $\sigma(\alpha) = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ for some $b_0, \ldots b_{n-1}$ in $M$. Then $\mu(\sigma(\alpha)) = b_0 + b_1\mu(\alpha) + \ldots + b_{n-1}\mu(\alpha)^{n-1}$. On the other hand since $\mu$ is a field automorphism fixing the minimal polynomial of $\alpha$, $\mu(\alpha) = \sigma^r(\alpha)$ for some $r < n$, hence $\sigma(\mu(\alpha)) = \sigma(\sigma^r(\alpha)) = \sigma^r(\sigma(\alpha)) = \sigma^r(b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}) = b_0 + b_1\sigma^r(\alpha) + \ldots + b_{n-1}\sigma^r(\alpha)^{n-1} = b_0 + b_1\mu(\alpha) + \ldots + b_{n-1}\mu(\alpha)^{n-1}$.

## 3. Geometric Representation

**Definition 2.** *We say that the group $G$ is* geometrically represented *in the theory $T$ if there exists $M_0 \prec M \vDash T$ and $M_0 \leq A \leq B \leq M$, such that $B \subseteq \mathrm{acl}(M)$ and $Aut(B/A) :\cong G$.*

In this definition, $A, B$ are substructures of $M$ containing $M_0$. $Aut(B/A)$ must be intepreted as the set of permutations of $B$ over $A$ preserving the truth value of all formulas (computed in $M$.)

In more detail, let $L_{Mor}$ be the Morleyzation, i.e. a language with a new relation symbol for each formula of $L$. Interpret the new relations symbols eponymously in $M$. By restriction we obtain $L_{Mor}$-structures on $A, B$, extending their $L$-structures. Now let $Aut(B/A)$ be the group of automorphisms of $B$ over $A$ as $L_{Mor}$-structures. For another approach to this definition, see [**H**].

**Definition 3.** *We say that a prime number $p$ is geometrically represented in the theory $T$ if there exists $M_0 \prec M \vDash T$ and $M_0 \leq A \leq B \leq M$, such that $B \subseteq \mathrm{acl}(M)$ and $\mathrm{Aut}(B/A) \cong \mathbb{Z}/p\mathbb{Z}$ or equivalently if $p||G|$ for some $G$ such that $G$ is geometrically represented in $T$.*

## 4. Maximal $p$-extensions

4.1. **Roots of Unity.** Let $k$ be a prime field of any characteristic and $p$ a prime $p \neq \mathrm{char}(k)$, we let $\mu_{p^n}$ denote the multiplicative subgroup of $K^a$ of $p^n$-th roots of unity. We also let $\mu_{p^\infty} = \bigcup_{n<\omega} \mu_{p^n}$.

It is a well-known fact that $\mathrm{Aut}(k(\mu_{p^\infty})/k)$ is the inverse limit of the automorphism groups of the finite extensions $\mathrm{Aut}(k(\mu_{p^n})/k)$ and that,

$$\mathrm{Aut}(k(\mu_{p^n})/k) \simeq \mathbb{Z}/p^{n-1}\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}.$$

Where $q = p - 1$ if $p \neq 2$ and $q = 2$ if $p = 2$.

For $i \geq j$, the restriction homomorphism

$$\begin{array}{rccc} r_{ij}: & \mathrm{Aut}(k(\mu_{p^i})/k) & \longrightarrow & \mathrm{Aut}(k(\mu_{p^j})/k) \\ & \phi & \longmapsto & \phi_{|k(\mu_{p^j})}, \end{array}$$

which is certainly onto, respects the decomposition. Hence

$$\mathrm{Aut}(k(\mu_{p^\infty})/k) \simeq \mathbb{Z}_p \times \mathbb{Z}/q\mathbb{Z}.$$

Let $L_p$ be the subfield of $k(\mu_{p^\infty})$ fixed by

$$\mathbb{Z}/q\mathbb{Z} < \mathbb{Z}_p \times \mathbb{Z}/q\mathbb{Z}$$

and let $\omega$ be a primitive $p$-th root of unity if $p \neq 2$ and $\sqrt{-1}$ if $p = 2$. The field $L_p$ does not contain any $p^n$-th roots of unity. Suppose it does then $L_p$ contains $\omega$ hence the automorphism group of $L_p/k$ contains a subgroup of index $q$ but it is impossible since $Aut(L_p/k) \simeq \mathbb{Z}_p$. But $L_p[\omega] = k(\mu_{p^\infty})$ and contains $\mu_{p^\infty}$.

In fact $L_p$ is the smallest subfield of $k(\mu_{p^\infty})$ that intersects $\mu_{p^\infty}$ trivially whereas the finite extension $L_p[\omega] = K(\mu_{p^\infty})$ contains all $p^n$-th roots of unity, it is the maximal abelian $p$-extension of $k$.

For a field $L$, $K \leq L$ and $A \subseteq L$, we will say that $K$ almost contains $A$ if $A$ is contained in a finite extension of $K$, i.e. $[K[A] : K] < \infty$.

We have the following result:

**Lemma 4.** *A field $K$ almost contains $\mu_{p^\infty}$ if and only if $L_p \subset K$.*

**Proof:** Suppose $K$ almost contains $\mu_{p^\infty}$ Let $k$ be the prime subfield of $K$ then

$$k_0 = k(\mu_{p^\infty}) \cap K$$

almost contains $\mu_{p^\infty}$ as well. So $\mathrm{Aut}(k(\mu_{p^\infty})/k_0)$ is a finite subgroup of $\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$. But a finite subgroup of $\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ has to be contained in $\mathbb{Z}/(p-1)\mathbb{Z}$. Therefore $k_0$, contains the fixed field of $\mathbb{Z}/(p-1)\mathbb{Z}$ in $k(\mu_{p^\infty})$ which is $L_p$ so does $K$. The converse of the lemma is trivial by definition. □

4.2. **Maximal $p$ extensions when $p = \mathrm{char}(k)$.** Given a field $F$ of characteristic $p$ we want to see the maximal $p$-extension of the prime field $\mathbb{F}_p$ inside $F$. The maximal $p$ extension of $\mathbb{F}_p$ in $F^a$ is equal to $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{p^n}}$. We will denote the maximal $p$ extension of $\mathbb{F}_p$ in $F$ which is $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^{p^n}} \cap F$ as $L_p$.

## 5. The Automorphism Group Theorem

In this section we will state and prove our main theorem on automorphism groups of pesudofinite fields. We will first prove the theorem for primes different from the characteristic of the pseudofinite field then we will extend the result to the primes equal to the characteristic.

**Theorem 5.** *Let $F$ be a quasifinite field, $p$ a prime different from* $\mathrm{char}(F)$*, and $\omega$ a primitive $p$-th root of unity. Assume (i) $p$ is geometrically represented in $Th(F)$. Then (ii) $F$ almost contains $\mu_{p^\infty}$. If $F$ is pseudo-finite, the converse holds.*

**Proof:** (i $\Rightarrow$ ii). Suppose $F$ contains substructures $A < B$ , $A$ containing an elementary submodule $M$ of $F$ and $p$ divides $|Aut(B/A)|$. Note that we may assume $B/A$ is a Galois extension of order $p$, generated by $\tau$, by replacing $A$ by $Fix(\tau)$ where $\tau$ is some element in $H$ of order $p$.

Without loss of generality we can assume that $\omega$ is in $F$ since $[A[\omega] : A] \mid p-1$, therefore the order of $\mathrm{Aut}(B[\omega]/A[\omega])$ is also $p$ and $F(\omega)$ is quasi-finite.

Since $F$ does not almost contain $\mu_{p^\infty}$, finite extension $F[\omega]$ of $F$ does not almost contain $\mu_{p^\infty}$ either. We have that $F[\omega]$ is a quasi-finite field containing substructures $A[\omega], B[\omega]$ with automorphism group $\mathrm{Aut}(B[\omega]/A[\omega])$ of order $p$, hence $F[\omega]$ satisfies condition (i) of the theorem. Since we assumed that $F$ contains the $p$-th roots of unity, by Kummer theory, $B = A[\delta]$ where $\delta^p = b$ for some $b$ in $A$. Let

$$C = \{x \in F^a \mid x^{p^n} = b, \text{ for some } n \in \mathbb{N}\}.$$

Note that $C$ is a $p$-divisible subset of $F^a$ and $\delta \in C$.

Claim: There exists some extension $\hat{\tau}$ of $\tau$ such that $\hat{\tau}$ fixes $A$ (and hence $b$) but acting nontrivially on $C$. Moreover, since $M$ is an elementary submodel of $F$, $M$ is relatively algebraically closed in $F$, $F$ and $M^a$ are linearly disjoint over $M$, and so we can choose a $\hat{\tau}$ which fixes the algebraic closure $M^a$ of the model $M$ contained in $A$. Remark here that $\hat{\tau}|F$ is an automorphism of $F$ since $\hat{\tau}$ commutes with $\sigma$ by Lemma 1, $\hat{\tau}$ sends the fixed field $F$ of $\sigma$ to itself.

An element $c \in C$ is a root of a polynomial $X^{p^n} - b$ over $A$ hence is $\hat{\tau}(c)$. Any two roots of $X^{p^n} - b$ differ by a $p^n$-th root of unity, hence $\hat{\tau}(c)/c \in \mu_{p^\infty}$ for every $c \in C$.

Define a multiplicative map $\phi$ from $C$ to $\mu_{p^\infty}$ as follows:

$$\begin{array}{rccc} \phi : & C & \longrightarrow & \mu_{p^\infty} \\ & c & \longmapsto & \hat{\tau}(c)/c. \end{array}$$

We claim that the image of $C$ is fixed by $\sigma$.

Recall that we choose $\hat{\tau}$ so that it fixes the algebraic closure $M^a$ of the model $M$ contained in $A$. Therefore, $\hat{\tau}$ fixes $\mu_{p^\infty}$. Suppose $\hat{\tau}(c) = \zeta_1 c$ and $\sigma(c) = \zeta_2 c$ for some $\zeta_1, \zeta_2$ in $\mu_{p^\infty}$. Then

$$\sigma(\hat{\tau}(c)/c) = \hat{\tau}(\sigma(c))/\sigma(c) = \hat{\tau}(\zeta_2 c)/(\zeta_2 c) = \hat{\tau}(c)/c.$$

Hence the image of $C$ is fixed by $\sigma$.

The part of $\mu_{p^\infty}$ fixed by $\sigma$ ($=\mu_{p^\infty} \cap F^*$) is a finite subgroup of $F^*$ since we assumed that $F$ does not contain $\mu_{p^\infty}$ and also that any nontrivial subgroup of $\mu_{p^\infty}$ is finite. Thus, the set $\{\hat{\tau}(c)/c\}_{c \in C}$ is finite.

Note that $C$ is $p$-divisible and also $\hat{\tau}(c^p)/c^p = (\hat{\tau}(c)/c)^p$, the image of $C$ under the map $\phi : c \rightarrow \tau(c)/c$ is $p$-divisible $p$-group. Then the finiteness of $\phi(C)$ implies that it must be trivial hence $\tau$ must fix $C$ which is a contradiction.

(ii $\Rightarrow$ i). For the converse, we may assume $F$ contains the $p^n$'th roots of unity. We assume that $Th(F)$ is pseudo-finite. So $Th(F)$ is the restriction to $Fix(\sigma)$ of a completion $T$ of the theory ACFA of algebraically closed fields with an automorphism $\sigma$. If $A$ is a substructure of a model of $T$ and $\text{acl}(A) = A$, it is known that any automorphism of $(A, \sigma)$ is elementary; in particular any automorphism $\tau$ of $(A, \sigma)$ restricts to an automorphism of $Fix(\sigma)$, elementary in the sense of $Th(F)$. We refer to [**CH**] for basic facts about ACFA.

Let $K$ be a countable subfield of $F$, containing the $p$'th roots of 1. Say $K = Fix(\sigma)$ where $(M, \sigma) \models T$. Let $N$ be the field of generalized power series in $x$ with $\mathbb{Q}$-exponents. By [**Ha**] this is an algebraically closed field, see [**K**]. Extend $\sigma$ to $N$ by mapping $\sum \alpha_i x^i$ to $\sum \sigma(\alpha_i) x^i$. Then $(N, \sigma)$ embeds into an elementary extension of $(M, \sigma)$.

Let $\{\omega_i\}_{i<\omega}$ be a coherent system of the $p$-th roots of unity in $K$, *i.e.* $\omega_0 = 1$ and $\omega_{i+1}^p = \omega_i$ for $i \geq 0$. Define $\tau$ to be an automorphism of $K^a((x^{1/n}))_{n \in \mathbb{N}}$ such that $\tau$ fixes $K^a$,

$$\tau : x^{1/p^i} \rightarrow \omega_i x^{1/p^i}$$

and

$$\tau : x^{1/n} \rightarrow x^{1/n} \text{ for } p \nmid n.$$

Note that, for $\sigma(x^{1/p^i}) = x^{1/p^i}$ we have that

$$\sigma(\tau(x^{1/p^i}) = \sigma(\omega_i x^{1/p^i}) = \omega_i x^{1/p^i}$$

$$\tau(\sigma(x^{1/p^i}) = \tau(x^{1/p^i}) = \omega_i x^{1/p^i},$$

hence $\sigma$ commutes with $\tau$ on $N$.

Since $\tau$ is defined on an algebraically closed field $K^a((x^{1/n}))_{n\in\mathbb{N}}$ we can extend $\tau$ to $F^a$ so that the extension commutes with $\sigma$. Hence $\tau$ restricts to an automorphism of the model $Fix(\sigma)$ of the theory $Th(F)$. Now, consider $A = K(x)$ and $B = K(x^{1/p})$ substructures of $F$ then $\mathrm{Aut}(K(x^{1/p})/K(x))$ is of order $p$ hence the claim is proved. □

## 6. When $p = \mathrm{char}(F)$

The following lemma is the key step in proving the theorem for characteristic of $F$ is $p$.

**Lemma 6.** *Let $A$ be an abelian group with three commuting operations acting $P, S, T$ acting on $A$. Let $A_0 = \cup_n \ker P^n$. Assume:*

(i) *$P$ is surjective.*
(ii) *$T|A_0 = 0$*
(iii) *$A_0 \cap \ker(S) \subseteq A_0 \cap \ker(P^N)$ for some $N$.*
*Then: if $a \in \ker(S)$ and $P(a) \in \ker(T)$, then $a \in \ker(T)$.*

**Proof:** Let $P(a) = b$ and $C = \{x \in A : P^n(x) = b \text{ for some } n > 0\}$. Since $S(b) = T(b) = 0$ we have $S(C)$, $T(C) \subseteq A_0$. By (2) $TS|_C = 0$ i.e. $T(C) \subseteq A_0 \cap \ker(S) \subseteq A_0 \cap \ker(P^N)$. But $C$ is $P$ divisible by definition and by (1), so $T(C)$ is $P$ divisible, hence $P^N$ divisible; so $T(C) = 0$.

**Theorem 7.** *[cont'd] Let $F$ be a quasi-finite field of characteristic $p$. Assume $F$ does not contain the maximal abelian $p$-extension $L_p$ of its prime field. Then $p$ is not geometrically represented in $Th(F)$.*

**Proof:** Suppose the maximal $p$ extension of $\mathbb{F}_p$ in $F$ is $\mathbb{F}_{p^{p^N}}$ for some $N$. Let $A, B$ substructures of $F$, $A$ definably closed containing an elementary submodel $M$ of $F$ such that $|\mathrm{Aut}(B/A)| = p$, then by Artin-Schreier theory there exists $b \in A$ such that $B = A(a)$ where $a^p - a = b$. Let $\tau$ be a generator of the Galois group $\mathrm{Aut}(B/A)$. Extend $\tau$ to an automorphism of $F^a$ fixing the algebraic closure of $\mathbb{F}_p$, this is possible since $\tau$ is fixing an elementary submodel of $F$. We will use Lemma 6 to get a contradiction. Let $A = F^+$ field $F$ with the additive structure, $P(x) = x^p - x$ $S = \sigma - \mathrm{Id}$ and $T = \tau - \mathrm{Id}$ acting on $F^a$ note that (i) $P$ is surjective on $F^a$ by algebraic closedness, (ii) $T|A_0 = 0$ since $\tau$ fixes the algebraic closure of an elementary submodel $M$, (iii) $A_0 \cap \ker(S) \subseteq A_0 \cap \ker(P^N)$ for some $N$ since we assumed that maximal $p$ extension of $\mathbb{F}_p$ in $F$ is $\mathbb{F}_{p^{p^N}}$ for some $N$. Then by construction $a \in F$, i.e. $a \in \ker(S)$, and $P(a) = b \in \ker(\tau)$, hence by the lemma any root $a$ of $x^p - x = b$ is in $\ker(\tau)$ hence fixed by $\tau$ which gives a contradiction. □

## 7. Automorphism Group and Tournaments

Let $p$ be a prime. By a *$p$-tournament* we mean a $p$-place relation $R$, such that for any $p$-tuple of distinct elements $x_1, \dots, x_p$,

$$R(x_{\tau(1)}, \dots, x_{\tau(p)}) \text{ holds for exactly one element } \tau \in < (12\dots p) >$$

where $(12\dots p)$ denotes the cyclic permutation of order $p$ over the $p$ element set $\{1, \dots, p\}$, and $< (12\dots p) >$ is the subgroup of $Sym(p)$ generated by this permutation, isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

A $p$-tournament clearly has no automorphism of order $p$, or even an automorphism $\sigma$ with a $p$-cycle $a_0, \dots, a_{p-1}$ with $\sigma(a_i) = a_{i+1} \bmod p$. Thus $p$ is *not* geometrically represented in $T$ if $T$ is 1-sorted and admits a $p$-tournament structure on the main sort. In fact no Galois group of $T$ can have order divisible by $p$, whether or not the base contains an elementary submodel.

**Proposition 8.** *Let $p$ be a prime, and $F$ a field of characteristic $\neq p$, containing the group $\mu_p$ of $p$'th roots of unity. Let $\omega \in \mu_p \setminus \{1\}$. Let $S$ be a set of representatives for the cosets of $\mu_p$ in $F^*$. Then in the structure $(F, +, \cdot, \omega, S)$ there exists a definable $p$-tournament on $F$.*

**Remark:** When $F$ is pseudo-finite, and $\omega \in F$, we have $[F^* : (F^*)^p] = p$ by a counting argument. The same conclusion holds when $F$ is quasi-finite, using Galois cohomology: the cohomology exact sequence associated with the short exact sequence

$$1 \to \mu_p \to (F^{alg})^* \to_{x \mapsto x^p} (F^{alg})^* \to 1$$

gives, using Hilbert 90,

$$F^* \to_{x \mapsto x^p} F^* \to Hom(\widehat{\mathbb{Z}}, \mu_p) \to H^1(Gal, (F^{alg})^*) = 0.$$

We refer to [**T**] for the basics of Galois cohomology.

Assume $F$ contains a primitive $p^n$-th root of unity $\zeta$, but not any $p$'th root of $\zeta$. Then $F^*$ is the direct sum of $\mu_{p^n}$ and $(F^*)^{p^n}$. Let $S_0$ be a set of representatives for $\mu_{p^n}/\mu_p$. Then $S_0(F^*)^{p^n}$ is a set of representatives for $(F^*)/\mu_p$. Hence, using the Proposition, there exists a $p$-tournament definable in the field $F$ using $\mu_{p^n}$ as parameters. This gives another proof of Theorem 6 (in the forward direction.)

Before proving Proposition 8, we illustrate it with the case $p = 2$. Assume $F$ does not contain $\sqrt{-1}$. A *tournament* on a set $X$ is an irreflexive binary relation $R \subset X \times X$ such that for every $x \neq y \in X$ exactly one of $R(x, y)$ and $R(y, x)$ holds. A pseudofinite field $F$ not containing $\sqrt{-1}$ interprets a tournament by the formula:

$$(\exists z)(z^2 = x - y).$$

The automorphism group of any field interpreting a 0-definable tournament can not have any involutions.

We can still define a tournament in a pseudofinite field $F$ which contains all the $2^n$-th roots of unity but not all the $(2^{n+1})$-st roots of unity.

For every $m \in \mathbb{N}$ we denote the set of $2^m$-th roots of unity by $\mu_{2^m}$. Let $S \subset \mu_{2^n}$, such that $S \cap -S = \emptyset$ and $S \cup -S = \mu_{2^n}$. Define a relation $R$ on $F \times F$ as follows:

$$R(x, y) \text{ if and only if } x - y \text{ is in } \bigcup_{c \in S} cF^{p^n}.$$

Then this defines a tournament in $F$. That is, for every $x, y \in F$, $x \neq y$, exactly one of $R(x, y)$ and $R(y, x)$ holds. Suppose $\neg R(x, y)$ then $(x - y) \notin \bigcup_{c \in S} cF^{2^n}$ then $(x - y)$ is in $\bigcup_{c \in -S} cF^{2^n}$. Therefore

$$-(x - y) = (y - x) \in \bigcup_{c \in S} cF^{2^n}$$

hence $R(y, x)$. Also, at most one of $R(x, y)$ and $R(y, x)$ hold since

$$F^{\times} = \bigsqcup_{c \in \mu_{2^n}} cF^{\times^{2^n}},$$

that is, $\mu_{2^n}$ is a set of representatives for the cosets of the subgroup $F^{\times^{2^n}}$ of multiplicative part $F^{\times}$ of $F$.

Now we will generalize the construcion of the above tournament relation from binary to $p$-ary.

**Proof:** of Proposition 8.

Define a $p$-ary relation $R_\omega$ on $F$ as follows:

$$R_\omega(x_1, x_2, \ldots, x_p) \text{ if and only if } x_1 + \omega x_2 + \ldots + \omega^{p-1} x_p \in S$$

**Claim:** 1 Assume $x_1 + \omega x_2 + \ldots + \omega^{p-1} x_p \neq 0$. Then

$$R_\omega(x_{\tau(1)}, \ldots, x_{\tau(p)}) \text{ holds for exactly one element in } <(12\ldots p)> \simeq \mathbb{Z}/p\mathbb{Z}.$$

Indeed let $\pi \in <(12\ldots p)>$ and $k = \pi(1)$ (so $k$ determines the element $\pi$). Then we have:

$$x_{\pi(1)} + \omega x_{\pi(2)} + \ldots + \omega^{p-1} x_{\pi(p)} = \omega^{k-1}(x_1 + \omega x_2 + \ldots + \omega^{p-1} x_p)$$

Since $S$ is a set of representatives for $F^*/\mu_p$, and $a := x_1 + \omega x_2 + \ldots + \omega^{p-1} x_p \in F^*$, it is clear that $\omega^{k-1} a \in S$ for a unique value of $k$ modulo $p$.

Thus $R_\omega$ is almost a $p$-tournament, but we need to deal with certain linearly dependent $p$-tuples.

**Claim:** 2 Assume $x_1 + \omega^i x_2 + \cdots + \omega^{i(p-1)} x_p = 0$ for all $i = 1, \ldots, p-1$. Then $x_1 = \cdots = x_p$.

This is because the Vandermonde matrix with rows $(1, \omega, \ldots, \omega^{p-1})$, $(1, \omega^2, \cdots, \omega^{2(p-1)})$, $\ldots$, $(1, \omega^{p-1}, \ldots, \omega^{((p-1)(p-1)}$ has rank $p-1$. So the kernel of this matrix is a vector space of dimension 1. But $(1, \ldots, 1)$ is clearly in the kernel; hence the kernel consists of scalar multiples of this vector.

Since we are only concerned with $p$-tuples of distinct elements, for each such $p$-tuple $x = (x_1, \ldots, x_p)$ there exists a smallest $i \in \{1, \ldots, p-1\}$ such that $x_1 + \omega^i x_2 + \ldots \neq 0$. Write $i = i(x)$, and define $R(x_1, \ldots, x_p)$ to hold iff $R_{\omega^{i(x)}}(x_1, \ldots, x_p)$ holds. It is then clear that $R$ is a $p$-tournament.

## 8. Model Theoretic Consequences

Let $T_{\mathrm{Psf}}$ be the theory of pseudo finite fields. Let $K = \mathbb{Q}$ or $K = \mathbb{F}_p$ By Ax's theorem [**Ax**] (cf. also [**FJ**], Chapter 20) is a one to one correspondence between the conjugacy classes of $\mathrm{Aut}(K^a/K)$ and the set of completions of the theory $T_{\mathrm{Psf}}$. Namely, note that $K^a \cap M$ is determined by $T$ up to isomorphism; call it $K^a_T$. Then $\sigma$ corresponds to $T$ iff $Fix(\sigma) \cong K^a_T$.

The absolute Galois group $\Gamma = Gal(K^a/K)$ is a compact topological group with a unique normalized left invariant Haar measure $\mu_\Gamma$. Let $\Pi$ be the set of conjugacy classes of $\Gamma$, and let $\pi : \Gamma \to \Pi$ be the quotient map. $\mu_\Gamma$ induces a measure $\mu$ on $\Pi$, namely $\mu(U) = \mu_\Gamma(\pi^{-1}(U))$. Using the 1-1 correspondence above, we identify $\Pi$ with the the set of completions $\mathcal{C}$ of the theory of pseudofinite fields of characteristic =char($K$). We obtain a measure on $\mathcal{C}$. By a theorem of Jarden (cf. Theorem 20.5.1 of [**FJ**]), for almost all $\sigma \in \Gamma$, $K^a_T \models T$.

**Corollary 9.** *For almost all $T$ in $\mathcal{C}$, we have $acl = dcl$ over $K^a_T$.*

**Proof:** For each $p \neq \mathrm{char}(F)$ the set $\{\sigma \in \mathrm{Aut}(F^a/F) : \sigma^{p-1} \text{ fixes } \mu_{p^\infty}\}$ has measure 0. So $\bigcup_{p \neq \mathrm{char}(F)} \{\sigma \in \mathrm{Aut}(F^a/F) : \sigma^{p-1} \text{ fixes } \mu_{p^\infty}\}$ has measure 0. If $\mathrm{char}(F) = p_0$, $\{\sigma \in \mathrm{Aut}(F^a/F) :$ $\sigma$ fixes the maximal $p_0$ extension $L_{p_0}\}$ has measure 0. Which implies, by Theorems 5 and 7, for almost all $T \in \mathcal{C}$ any group which is geometrically represented in $T$ is trivial, hence $acl = dcl$ over $K^a_T$.

**Remarks:**

We remark that while dcl = acl is a restricted form of Skolemization, the theories of pseudo-finite fields are not Skolemized. For instance, let $F_0$ be pseudo-finite $\mathrm{char}(F_0) = 0$, and let $K = F_0((t^{\mathbb{Q}}))$ be the field of Puiseux series over $F_0$. Then $K$ has Galois group $\hat{\mathbb{Z}}$, and embeds into a pseudo-finite field $F$ such that $Aut(F^a/F) \to Aut(K^a/k)$ is an isomorphism; hence $K$ is relatively algebraically closed in $F$. But being Henselian and non-separably closed it cannot be PAC, by Corollary 11.5.6 of [**FJ**].

It would be interesting to know which finite groups can be geometrically represented in theories of pseudo-finite fields.

## References

[**Ax**] Ax, J. "The elementary theory of finite fields", *Ann. Math.* **88** (1968) 239-271.

[**CH**] Chatzidakis, Z. Hrushovski, E. "Model theory of difference fields", *Trans. Amer. Math. Soc.* **351** (1999), no. 8, 2997–3071.

[**FJ**] Fried, M. Jarden, M. *Field Arithmetic*, Erg. Math. **11**, Springer-Verlag Berlin, 2005.

[**Ha**] Hahn, H. "Über die nichtarchimedischen Grössensysteme", Sitzungsberichte der Kaiserlichen Akademie der Wissenschaften, Wien, Mathematisch - Naturwissenschaftliche Klasse (Wien. Ber.) (1907),116: 601655 (reprinted in: Hahn, Hans (1995). Gesammelte Abhandlungen I. Springer-Verlag. )

[**H**] Hrushovski, E., "Finitely Axiomatizable Aleph-One Categorical Theories", *Journal of Symbolic Logic*, **59** (1994) pp. 838-845

[**K**] Kedlaya, Kiran Sridhara, "The algebraic closure of the power series field in positive characteristic", Proc. Amer. Math. Soc. **129** (2001) pp. 34613470

[**S**] Serre, Jean-Pierre *Local Fields.* New York: Springer Verlag, 1979.

[**S**] Serre, Jean-Pierre *Galois Cohomology.* Berin: Springer Verlag, 1997.

[**T**] Tate, J. *Galois Cohomology* [Internet], IAS/ Parkcity Mathematics Series; 1999 [cited 2009, August 25]. Available from: http://modular.math.washington.edu/Tables/Notes/tate-pcmi.html